27 July 2015

# NORTH DAKOTA

# HOMELAND SECURITY

# Cyber Summary

**The North Dakota Open Source Cyber Summary is a product of the North Dakota State and Local Intelligence Center (NDSLIC). It provides open source news articles and information on terrorism, crime, and potential destructive or damaging acts of nature or unintentional acts. Articles are placed in the Cyber Summary to provide situational awareness for local law enforcement, first responders, government officials, and private/public infrastructure owners.**

## NDSLIC Disclaimer

The Cyber Summary is a non-commercial publication intended to educate and inform. Further reproduction or redistribution is subject to original copyright restrictions. NDSLIC provides no warranty of ownership of the copyright, or accuracy with respect to the original source material.

## Table of Contents

## North Dakota

**Nothing Significant to Report**

## Regional

**Nothing Significant to Report**

## National

(National) **Extremist groups use social media to lure recruits, find support.** In the past, extremist groups have used tools and forums which were available: Rallies, pamphleteering, and marching in parades were the primary means used for recruitment and spreading their message. Now, as is the case with many other individuals and groups, these efforts have adapted to more contemporary media to target college and university campuses, to gain new members or, at least, sympathy to their cause. They now use the Internet to conduct forums and publish newsletters, a method that exposes potentially millions to their message. http://www.homelandsecuritynewswire.com/dr20150720-extremist-groups-use-social-media-to-lure-recruits-find-support

## International

(International) **Attacks on Critical Infrastructure Organizations Resulted in Physical Damage: Survey.** A total of 625 IT decision makers from public and private critical infrastructure organizations in the United States, France, Germany and the United Kingdom took part in a survey conducted by Vanson Bourne. The survey has found that while critical infrastructure security experts agree that attack volume, number of breaches, and the rate of vulnerable code are increasing, many of the respondents stated that their own organizations have become less vulnerable. Only 27 percent of respondents said they feel very or

extremely vulnerable today. In comparison, 50 percent of them stated that they felt this way three years ago.
http://www.securityweek.com/attacks-critical-infrastructure-organizations-resulted-physical-damage-survey?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+Securityweek+%28SecurityWeek+RSS+Feed%29&utm_content=FeedBurner

**(International) Study: half of critical infrastructure IT professionals believe major attack looming.** Findings from a survey of over 600 critical infrastructure information technology (IT) professionals in Intel Security's "Critical Infrastructure Readiness Report" revealed that about half of all respondents believe an attack on critical infrastructure in the next three years will down systems and lead to loss of life, and that 90 percent of respondents' organizations faced an average of 20 attacks in the last year, among other statistics.
http://www.scmagazine.com/intel-security-conducts-cyberattack-survey/article/427429/

**(International) North Wales wants to be "one of the most secure places in the world to do business".** Glyndŵr University is to play a leading role in the fight against cybercrime. The Wrexham, Wales-based university hosted the first meeting of the North Wales Cyber Security Cluster on Thursday (23 July). The institution and North Wales Police saw experts in online security and e-crime join the forum, and also invited members of the public and business owners who have been targeted in the past to attend and share information and advice, in a bid, the organizers say, "to make North Wales one of the most secure places in the world to do business."
http://www.homelandsecuritynewswire.com/dr20150724-north-wales-wants-to-be-one-of-the-most-secure-places-in-the-world-to-do-business

**(International) Journalists' computer security tools lacking in a post-Snowden world.** Edward Snowden's leak of classified documents to journalists around the world about massive government surveillance programs and threats to personal privacy ultimately resulted in a Pulitzer Prize for public service. Though Snowden had no intention of hiding his identity, the disclosures also raised new questions about how effectively news organizations can protect anonymous sources and sensitive information in an era of constant data collection and tracking.

Researchers found a number of security weaknesses in journalists' and news organizations' technological tools and ad-hoc workarounds.
http://www.homelandsecuritynewswire.com/dr20150724-journalists-computer-security-tools-lacking-in-a-postsnowden-world

## Banking and Finance Industry

**Nothing Significant to Report**

## Chemical and Hazardous Materials Sector

**Nothing Significant to Report**

## Commercial Facilities

**(International) Google, Security Firms Warn About Impact of Wassenaar Cybersecurity Rules.** Several leading cybersecurity firms have formed a coalition whose goal is to prevent the U.S. Department of Commerce from adopting Wassenaar Arrangement regulations that could have a negative impact on the industry. The Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies is a multilateral export control association with 41 participating states. Members have agreed to control the transfer of arms and dual-use goods and technologies in an effort to improve national and international security and stability. Google believes the proposed changes would have a significant negative impact on the open security research community. The company is also concerned that the rules would affect its ability to defend itself and its customers.
http://www.securityweek.com/google-security-firms-warn-about-impact-wassenaar-cybersecurity-rules

## Communications Sector

**Nothing Significant to Report**

## Critical Manufacturing

(International) **All Smartwatches Vulnerable to Attack: HP Study**. HP this week shared the results of a security assessment revealing that virtually all smartwatches with network and communication functionality are vulnerable to cyberattacks. The study found that 100 percent of the tested smartwatches contain significant vulnerabilities, including poor authentication, lack of encryption and privacy issues. HP said that it evaluated 10 of the top smartwatches currently on the market, along with their Android and iOS apps, from an attacker's perspective.
http://www.securityweek.com/all-smartwatches-vulnerable-attack-hp-study

## Defense/ Industry Base Sector

**Nothing Significant to Report**

## Emergency Services

**Nothing Significant to Report**

## Energy

(National) **Cyber Attack on Power Grid Could Top $1 Trillion in Damage.** Lloyd's and the Cambridge Centre for Risk Studies at University of Cambridge Judge Business School examined the implications of a fictional attack where adversaries damaged 50 generators supplying power to the electrical grid and caused a blackout across 15 states along the East Coast and Washington D.C. and affected

93 million people. Lloyd's produced the Business Blackout report to help insurance underwriters understand how cyberattacks impact insurance and risk. http://www.securityweek.com/cyber-attack-power-grid-could-top-1-trillion-damage-report?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+Securityweek+%28SecurityWeek+RSS+Feed%29

## Food and Agriculture

**Nothing Significant to Report**

## Government Sector (including Schools and Universities)

(National) **Fusion Centers important in promoting cybersecurity**. Fusion centers were created after 9/11 to serve as primary focal points for state, local, federal, tribal, and territorial partners to receive, analyze, and share threat-related information. States can promote cybersecurity and enhance their capabilities by heightening the importance of cybersecurity as a mission of fusion centers, according to a paper released the other day by the National Governors Association (NGA). http://www.homelandsecuritynewswire.com/dr20150721-fusion-centers-important-in-promoting-cybersecurity

(National) **OPM changes privacy rules to let investigators inside all databases.** The U.S. Office of Personnel Management announced July 16 updated privacy regulations for routine use, granting access for investigators to all its databases in the case of suspected or confirmed security breaches. The public has until August 17 to comment on these changes in confidentiality. http://www.nextgov.com/cybersecurity/2015/07/opm-changes-privacy-rules-let-investigators-inside-all-databases/118105/

(National) **Security experts point to OPM's biggest cybersecurity failure.** The Institute for Critical Infrastructure Technology released a report citing the lack of a comprehensive governing policy for cybersecurity as the greatest failure leading to the June breach of its systems, and recommended that the agency address security gaps identified by auditors and implement a behavioral analytics system to compensate for rapidly advancing advanced persistent, sophisticated threats. http://www.nextgov.com/cybersecurity/2015/07/security-experts-point-opms-biggest-cybersecurity-failure/118274/

(National) **Proposed bill would formalize DHS role in securing government networks**. The hacking of the federal Office of Personnel Management (OPM), which resulted in the theft of records of twenty-two million federal employees and their families, has prompted a Senate response. A bipartisan group of U.S. senators has introduced a bill on the heels of that event, updating the original Federal Information Security Management Act (FISMA) and formalizing the role of DHS in securing government networks and Web sites. http://www.homelandsecuritynewswire.com/dr20150724-proposed-bill-would-formalize-dhs-role-in-securing-government-networks

(National) **Census Bureau confirms 'unauthorized access' to system; Anonymous members claim responsibility.** The online activist group Anonymous claimed responsibility July 22 for a cyber-attack on the U.S. Census Bureau, which leaked non-confidential information including email addresses, phone numbers, and job titles of the organization's 4,200 employees. The organization's internal systems were not affected, and the compromised servers have been locked down. http://www.fiercegovernmentit.com/story/census-bureau-confirms-unauthorized-access-system-anonymous-claims-responsi/2015-07-23

## Information Technology and Telecommunications

(International) **Ashley Madison hacked, info of 37million users stolen.** Hackers calling themselves "The Impact Team" reportedly accessed and stole personal information and financial records of 37 million of AvidLife's Ashley Madison Web site as well as user databases for 2 other sites that the company owns. The hack was perpetrated in response to Avid Life's failure to provide its offered "full delete" feature for user profiles.

http://www.net-security.org/secworld.php?id=18643

(International) **Configuration Issue Exposes 30,000 MongoDB Instances**
The founder of the Shodan computer search engine reported that a default listening configuration in MongoDB exposed about 30,000 database instances containing 592.2 terabytes (TB) of data.
http://www.securityweek.com/configuration-issue-exposes-30000-mongodb-instances-researcher

(International) **It's official: the average DDoS attack size is increasing.** Arbor Networks reported analysis from Quarter 2, 2015 global distributed denial-of-service (DDoS) attack data revealing that the average size of attacks increased, and that the majority of large volumetric attacks leveraged Network Time Protocol (NDP), Simple Service Discovery Protocol (SSDP), and Domain Name System (DNS) servers for reflecting amplification, among other findings.
http://www.net-security.org/secworld.php?id=18651

(International) **Researcher discloses local privilege escalation vulnerability in OS X.** Security researchers from SektionEins released details on a vulnerability in Mac Operating System (OS) X in which an attacker could open or create arbitrary files owned by the root user anywhere in the file system by leveraging an environmental variable that enables error logging to arbitrary files.
http://www.securityweek.com/researcher-discloses-local-privilege-escalation-vulnerability-os-x

(International) **Bug exposes OpenSSH servers to brute-force password guessing attacks.** Security researchers reported that OpenSSH servers with keyboard-interactive authentication enabled by default are vulnerable to unlimited authentication retries over a single connection, exposing users to brute-force password guessing attacks.
http://www.networkworld.com/article/2951493/bug-exposes-openssh-servers-to-bruteforce-password-guessing-attacks.html#tk.rss_all

(International) **Red Hat patches "libuser" library vulnerabilities.** Red Hat patched two vulnerabilities in its "libuser" library, including a race condition flaw that could lead to a denial-of-service (DoS) condition and a bug in the chfn function of the user helper utility that an attacker could leverage to create a DoS condition and achieve privilege escalation on the system.

http://www.securityweek.com/red-hat-patches-%E2%80%9Clibuser%E2%80%9D-library-vulnerabilities

## US-Cert Updates and Vulnerabilities

**(International) Update: Microsoft Releases Security Update.** This security update resolves a vulnerability in Microsoft Windows. The vulnerability could allow remote code execution if a user opens a specially crafted document or visits an untrusted webpage that contains embedded OpenType fonts. This security update is rated Critical for all supported releases of Microsoft Windows. https://www.us-cert.gov/ncas/current-activity/2015/07/20/Microsoft-Releases-Security-Update

**(National) Update: WordPress Releases Security Update.** WordPress 4.2.2 and prior versions contain critical cross-site scripting vulnerabilities. Exploitation of these vulnerabilities could allow a remote attacker to take control of an affected website.
https://www.us-cert.gov/ncas/current-activity/2015/07/23/WordPress-Releases-Security-Update

**(National) Update: Cisco Releases Security Updates.** Cisco has released security updates to address vulnerabilities in its Application Policy Infrastructure Controller, IOS software, and the Unified MeetingPlace Conferencing products. Exploitation of these vulnerabilities may allow a remote attacker to gain unauthorized access, cause a denial-of-service condition, or take control of the affected application. https://www.us-cert.gov/ncas/current-activity/2015/07/23/Cisco-Releases-Security-Updates

**(International) Update: Google Chrome update includes 43 security fixes.** Google released an update for Chrome addressing 43 heap-buffer-overflow, use-after-free, and memory corruption vulnerabilities, among others, that could allow an attacker to take control of an affected system.
http://www.net-security.org/secworld.php?id=18652

(International) **Honeywell Tuxedo Touch Controller contains multiple vulnerabilities.** All versions of Honeywell Tuxedo Touch Controller are vulnerable to authentication bypass and cross-site request forgery (CSRF). A remote, unauthenticated attacker may be able to bypass authentication checks to view restricted pages, or trick an authenticated user into making an unintentional request to the web server which will be treated as an authentic request. Compromised Tuxedo Touch Controllers may be leveraged to operate home automation devices, such as unlocking or locking doors. The solution to this vulnerability is to apply firmware update version TUXW_V5.2.19.0_VA, http://www.kb.cert.org/vuls/id/857948

## ICS-Cert Alerts and Advisories

(International) **Advisory: Hospira Symbiq Infusion System Vulnerability.** Independent researcher Billy Rios identified a vulnerability in Hospira's Symbiq Infusion System, which can be exploited to remotely control the device, in conjunction with previously identified vulnerabilities.[a] Kyle Kamke of Ramparts LLC assisted in the development of the proof-of-exploit. Hospira has verified that this vulnerability only exists in the Symbiq Infusion System. Hospira has provided compensating measures to help mitigate risks associated with this vulnerability. As previously announced by Hospira in 2013, the Symbiq Infusion System would be retired on May 31, 2015, and will be fully removed from the market by December 2015.This vulnerability could be exploited remotely. https://ics-cert.us-cert.gov/advisories/ICSA-15-174-01

(International) **Advisory: Siemens RuggedCom ROS and ROX-based Devices TLS POODLE Vulnerability.** Siemens has reported to NCCIC/ICS-CERT that a Transport Layer Security (TLS) Padding Oracle On Downgraded Legacy Encryption (POODLE) vulnerability exists in the web interface of Siemens RuggedCom ROS and ROX-based devices. Siemens has produced a firmware update to mitigate this vulnerability. This vulnerability could be exploited remotely. https://ics-cert.us-cert.gov/advisories/ICSA-15-202-03A

(International) **Advisory: Siemens Sm@rtClient Password Storage Vulnerability.** Siemens has identified a password storage vulnerability in its Sm@rtClient Android application. This vulnerability was reported directly to Siemens by Karsten Sohr from Universität Bremen and Stephan Huber from Fraunhofer SIT. Siemens has produced a new version to mitigate this vulnerability. This vulnerability can only be exploited locally.
https://ics-cert.us-cert.gov/advisories/ICSA-15-202-02

(International) **Advisory: Siemens SIPROTEC Denial-of-Service Vulnerability.** Siemens has identified a denial-of-service vulnerability in the SIPROTEC 4 and SIPROTEC Compact devices. This vulnerability was reported directly to Siemens by Victor Nikitin from i‑Grids LLC Russia. Siemens has produced a new firmware update to mitigate this vulnerability. This vulnerability could be exploited remotely.
https://ics-cert.us-cert.gov/advisories/ICSA-15-202-01

(National) **Alert: FCA Uconnect Vulnerability**. NCCIC/ICS-CERT is aware of a public report and video of researchers demonstrating remote exploits on a magazine reporter's automobile. The report and video are available at: http://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/. The report and video focus on unauthorized remote access to the Fiat Chrysler Automobile (FCA) Connect automotive infotainment system. According to this report, the vulnerability is exploitable by leveraging known VIN information to the Uconnect system via the Sprint network. The report itself claims the researchers have been sharing this research with FCA for nearly 9 months. FCA released a security notice and a firmware patch to owners of vehicles with the Uconnect feature on July 16, 2015. ICS-CERT is issuing this alert to provide notice of this report and video, and that a patch is available from the FCA.
https://ics-cert.us-cert.gov/alerts/ICS-ALERT-15-203-01\

## Public Health

(International) **CVS investigating possible payment card breach, shuts down photo Web site.** CVS reported that the company had shut down its CVSPhoto.com Web site while it investigated a possible payment card beach of the independent vendor that manages and hosts the site, PNI Digital Media. Company officials

confirmed that purchases made in-store and on other CVS Web pages are not affected.
http://www.scmagazine.com/cvs-investigating-possible-payment-card-breach-shuts-down-photo-website/article/427116/

(National) **4.5 Million Individuals Exposed in UCLA Health Breach.** According to a notice published on Friday by the healthcare organization, the breach was discovered in October 2014. The FBI and a team of computer forensics experts were called in by UCLA Health to assist with the investigation and response process. While initially it did not appear that the attackers had gained access to parts of the UCLA Health network containing personal and medical information, on May 5, 2015 investigators determined that sensitive parts of the network had in fact been compromised.
http://www.securityweek.com/details-45-million-individuals-exposed-ucla-health-breach?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+Securityweek+%28SecurityWeek+RSS+Feed%29&utm_content=FeedBurner

(National) **Why Healthcare Security Matters.** Medical records can be worth as much as 10 times more than credit card numbers on the black market. Attackers are using the information to buy medical equipment or drugs that can be resold or to file fraudulent claims with insurers.
http://www.securityweek.com/healthcare-security-matters

## Transportation

(International) **The Ever-evolving Cyber Threat to Planes.** Most agree hacking a plane would be a near-impossible feat, but some professional hackers have claimed airline computer systems are riddled with weaknesses that could allow someone to break in, perhaps even through the in-flight entertainment system.
http://www.securityweek.com/ever-evolving-cyber-threat-planes

(International) **Firewalls can't protect today's connected cars.** Security and automotive experts reported on the risks associated with Internet-enabled vehicles, including a lack of operational security and multiple access wireless access points to vehicles' controller area networks (CAN). The researchers

recommended alternate approaches to vehicle security such as encrypted CAN messaging or detection-software.
http://www.networkworld.com/article/2951888/security/firewalls-cant-protect-todays-connected-cars.html#tk.rss_all

## Water and Dams

**Nothing Significant to Report**

## North Dakota Homeland Security Contacts

**To report a homeland security incident, please contact your local law enforcement agency or one of these agencies: North Dakota State and Local Intelligence Center: 866-885-8295(IN ND ONLY); Email: ndslic@nd.gov; Fax: 701-328-8175 State Radio: 800-472-2121; Bureau of Criminal Investigation (BCI): 701-328-5500; North Dakota Highway Patrol: 701-328-2455; US Attorney's Office Intel Analyst: 701-297-7400; Bismarck FBI: 701-223-4875; Fargo FBI: 701-232-7241.**

**To contribute to this summary or if you have questions or comments, please contact:**

**Darin Hanson, ND Division of Homeland Security dthanson@nd.gov, 701-328-8165**